FORM PTO-1390 REV. 5-93	US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER P00,1996
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S. APPLICATION NO. (if known, see 37 CFR 1.5) 09/763271
INTERNATIONAL APPLICATION NO. **PCT/DE99/02443**	INTERNATIONAL FILING DATE **04 AUGUST 1999**	PRIORITY DATE CLAIMED **18 AUGUST 1998**

TITLE OF INVENTION

METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

APPLICANT(S) FOR DO/EO/US **GERHARD HOFFMANN ET AL**

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)) - drawings attached.
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2) - drawings attached.

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report, 06 References).**

12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**

13. ☒ Amendment "A" Prior to Action and Appendix "A".
    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☒ A substitute specification and substitute specification mark-up.

15. ☒ A change of address letter attached to the Declaration.

16. ☒ Other items or information:
    a. ☒ Drawing Changes

    b. ☒ Appointment of Associate Power of Attorney

    c. ☒ EXPRESS MAIL #EL655300859US dated February 20, 2001

U.S. APPLICATION NO. (if known, see 37 C.F.R. 1.5) 09/763271	INTERNATIONAL APPLICATION NO. PCT/DE99/02443	ATTORNEY'S DOCKET NUMBER P00,1996

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5): Search Report has been prepared by the EPO or JPO $860.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) . . $690.00		
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) $710.00		
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $1000.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . . $ 100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

Claims	Number Filed		Number Extra	Rate		
Total Claims	20	- 20 =	0	X $ 18.00	$	
Independent Claims	02	- 3 =	0	X $ 80.00	$	
Multiple Dependent Claims				$270.00+	$	
TOTAL OF ABOVE CALCULATIONS =					$ 860.00	
Reduction by ½ for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)					$	
SUBTOTAL =					$ 860.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					$	
TOTAL NATIONAL FEE =					$ 860.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +						
TOTAL FEES ENCLOSED =					$ 860.00	
					Amount to be refunded	$
					charged	$

a. ☒ A check in the amount of $ 860.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1519. **A duplicate copy of this sheet is enclosed.**

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
SCHIFF HARDIN & WAITE
PATENT DEPARTMENT
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473

CUSTOMER NUMBER 26574

Mark Bergner
SIGNATURE

Mark Bergner
NAME

45,877
Registration Number

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

PRELIMINARY AMENDMENT A
PRIOR TO ACTION

APPLICANT(S):	GERHARD HOFFMANN ET AL
ATTORNEY DOCKET NO.:	P00,1996
INTERNATIONAL APPLICATION NO:	PCT/DE99/02443
INTERNATIONAL FILING DATE:	04 AUGUST 1999
INVENTION:	METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

Assistant Commissioner for Patents,
Washington D.C. 20231

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE CLAIMS:

On page 13:

replace line 1 with --WHAT IS CLAIMED IS:--;

Please replace original claims 1-20 with the following rewritten claims 1-20, referring to the mark-ups in Appendix A.

1. (Amended) A method for forming a secret communication key for a predetermined asymmetric cryptographic key pair which comprises a private key and a corresponding public key, by a computer, comprising the steps of:

utilizing a prescribable initial value given a determination of said key pair;

providing said initial value to a user;

entering, by said user, said initial value into said computer; and

forming said secret communication key upon utilization of said initial value, said secret communication key and said public key forming an asymmetric cryptographic communication key pair.

2. (Amended) The method according to claim 1, further comprising the steps of:

supplying said initial value to a hash function; and

determining, using a hash function value formed by said hash function, said key pair and said communication key pair.

3. (Amended) The method according to claim 1, further comprising the step of:

including additional data characterizing said user when said key pair and said communication key pair are formed.

4. (Amended) The method according to claim 1, further comprising the steps of:

determining a prime number based on said initial value, where, in an iterative method, the following steps are performed:

checking said initial value or a previously checked number, producing a checked number, to determine whether said checked number is a prime number and (determination of primacy), and if said checked number is a prime, storing an index, which refers to a plurality of numbers, which have been checked with respect to their property of being prime; and

selecting, when said number is not a prime number, another number based on said checked number and said index, said checked number being increased by a prescribed number;

said method further comprising the steps of:

erasing a used prime number after said communication key pair has been formed; and

forming, with said index and said initial value, a new communication key pair for forming said secret communication key.

5. (Amended) The method according to claim 4, wherein said determination of primacy for any given number is carried out according to the method of Miller-Rabin.

6. (Amended) The method according to claim 1 wherein keys are formed according to the RSA method.

7. (Amended) The method according to claim 2 wherein said hash function is selected from the group consisting of the methods MD-5 method, the MD-2 method, and the Data Encryption Standard (DES) method as a one-way function.

8. (Amended) The method according to claim 1, further comprising the step of:

enciphering electronic data with said secret communication key.

9. (Amended) The method according to claim 1, further comprising the step of:

forming a digital signature via electronic data using said secret communication key.

10. (Amended) The method according to claim 1, further comprising the step of:

authenticating data using said secret communication key.

11. (Amended) An arrangement for forming a secret communication key for a

predetermined asymmetric cryptographic key pair which comprises a private key and a corresponding public key, comprising:

an input device configured for entering an initial value by a user; and

a processor connected to said input device, said processor configured to:

determine, using said prescribable initial value, said asymmetric cryptographic key pair;

accept entry of said initial value made available to said user; and

form said secret communication key using said initial value, where said secret communication key and said public key form a communication key pair.

12. (Amended) The arrangement according to claim 11, wherein said processor is configured such that said initial value is supplied to a hash function and a hash value formed by the hash function is used for determining said asymmetric cryptographic key pair and the communication key pair.

13. (Amended) The arrangement according to claim 11, wherein said processor is configured such that additional data characterizing said user are utilized during said formation of said asymmetric cryptographic key pair and said communication key pair.

14. (Amended) The arrangement according to claim 11, wherein said processor is configured to:

determine a prime number based on said initial value, where, in an iterative method:

said initial value or a previously checked number is checked, producing a checked number, to determine whether said checked number is a prime number (determination of primacy), and if said checked number is a prime, storing an index, which refers to a plurality of numbers, which have been checked with respect to their property of being prime; and

select, when said number is not a prime number, another number

based on said checked number and said index, said checked number being increased by a prescribed number;

said processor further being configured to:

erase a used prime number after said communication key pair has been formed; and

form, with said index and said initial value, a new communication key pair for forming said secret communication key.

15. (Amended) The arrangement according to claim 14, wherein said processor is configured carry out said determination of primacy according to the method of Miller-Rabin.

16. (Amended) The arrangement according to claim 11, wherein said processor is configured to form keys according to the RSA method.

17. (Amended) The arrangement according to claim 12, wherein said processor is configured to produce said hash function according to a method selected from the group consisting of the MD-5 method, the MD-2 method, and the Data Encryption Standard (DES) method as one-way function.

18. (Amended) The arrangement according to claim 11 used for enciphering electronic data with said secret communication key.

19. (Amended) The arrangement according to claim 11 used for forming a digital signature via electronic data upon utilization of said secret communication key.

20. (Amended) The arrangement according to claim 11 used for authenticating data upon utilization of said secret communication key.

REMARKS

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. Pursuant to 37 CFR 1.125 (b), applicants have concurrently submitted a substitute specification, excluding the claims, and provided a marked-up copy. All of the changes are editorial and applicant believes no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested.

Submitted by,

Mark Bergner (Reg. No. 45,877)

Mark Bergner
Schiff Hardin & Waite
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473
(312) 258-5779
Attorneys for Applicant

CUSTOMER NUMBER 26574

SPECIFICATION

TITLE

METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

BACKGROUND OF THE INVENTION

Field of the Invention

1 The invention relates to a method and an arrangement for forming a secret communication key for a predetermined asymmetric key pair.

Description of the Related Art

2 The formation of an asymmetric cryptographic key pair is known from C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 79 - 85, 1993 (Ruland I), which discloses the RSA method for forming a cryptographic key pair, which comprises a secret (private) key and a corresponding public key. Only the user knows the private key, but the public key can be made known to all subscribers of a communication network. In this method, the user signs the data with his private key when a digital signature is prepared for protecting the authenticity and integrity of electronic data. The signed digital signature is verified upon utilization of the public key corresponding to the private key, so that the authenticity or integrity of the digital signature can be checked by all communication partners, who have access to the public key. The previously mentioned "Public-Key-Technology" is particularly applied in the digital communication within a computer network (a fixed number of computer units, which are connected to one another via a communication network). Given the method known from Ruland, the protection of the private key against unauthorized access of a third party is of critical importance for the security of the digital signature.

3 It is known from D. Longley and M. Shain, Data & Computer Security, Dictionary of standards concepts and terms, Stockton Press, ISBN 0-333-42935-4, page 317, 1987 (Longley) to store the private key on an external medium for storing data, for example, a chip card, a disk etc., or on a hard disk, where key data are protected in that a personal identification code (Personal Identification Number, PIN)

SUBSTITUTE SPECIFICATION

or a password, with which the key data that are respectively deciphered is used. It is necessary, however, to access the local resources of a user when these external media are used. This is not desired especially with respect to a network-oriented infrastructure of network computers or Java applications. These are defined as follows. A network computer is a computer that is networked with other computers; and a Java application is a program containing programs that are written in the programming language Java. The method known from Longley is disadvantageous in that the private key must be stored on an external medium, so that it is very difficult to protect the private key against misuse.

4 An overview regarding hash functions can be found in C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 68 - 73, 1993 (Ruland II). A hash function is a function in which it is possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function, such as collision freedom, which precludes the possibility of finding two different input character strings resulting in the same output character string. Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

5 A method referred to as a "Miller-Rabin" can determine whether a number is prime or not. Such a method is known from A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN 0-8493-8523-7, page 138 - 140, 1997 (Menezes).

SUMMARY OF THE INVENTION

6 An object of the invention is to form a secret communication key for a predetermined asymmetric cryptographic key pair, where the private key of the asymmetric key pair must not be stored permanently.

7 The problem is solved by a method for forming a secret communication key for a predetermined asymmetric cryptographic key pair which comprises a private

key and a corresponding public key, by a computer, comprising the steps of utilizing a prescribable initial value given a determination of the key pair; providing the initial value to a user; entering, by the user, the initial value into the computer; and forming the secret communication key upon utilization of the initial value, the secret communication key and the public key forming an asymmetric cryptographic communication key pair.

8 The problem is also solved by an arrangement comprising an input device configured for entering an initial value by a user; and a processor connected to the input device, the processor configured to implement the above method.

9 Given the method for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a private key and a corresponding public key, a prescribable initial value (that is available to a user) is used with respect to the determination of the key pair. The user enters the initial value into the computer and the secret communication key is formed upon utilization of the initial value. The secret communication key and the public key form a communication key pair, which is not to be confused with the predetermined asymmetric cryptographic key pair.

10 The arrangement for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a private key and a corresponding public key, has a processor, which is set up such that the following steps can be carried out:

- a prescribed initial value is used for determining the key pair,
- the user enters the initial value into the computer,
- the secret communication key is formed upon utilization of the initial value, where the secret communication key and the public key form a communication key pair.

11 Furthermore, an input device is provided for entering the initial value by the user.

12 As a result of the invention, it is possible to erase the private key without having to forego the intense cryptography of the "Public-Key-Technology".

Concretely, the initial value can be regarded as a personal identification code (Personal Identification Number- PIN) or as a password that is prescribed by the user or that is centrally prescribed and that is entered by the user into the computer. After the password or the PIN has been entered, the secret communication key, i.e., the key that is of the same name compared to the private key, is formed, which forms a communication key pair together with the public key (i.e., the communication key pair comprises the public key and the secret communication key), upon utilization of the password or of the PIN as an initial value.

13 In this way, a fusion of the password technology customary to the user of a conventional computer network or of a conventional computer with the intense cryptology is inventively achieved without considerable efforts being necessary in order to permanently store private key material.

14 Preferred embodiments of the method and associated apparatus for implementing the method are provided as follows. The inventive method may further comprise the steps of: supplying the initial value to a hash function; and determining, using a hash function value formed by the hash function, the key pair and the communication key pair. The formation of the communication key pair may further include additional data characterizing the user. The method may further comprise the steps of: determining a prime number based on the initial value, where, in an iterative method, the following steps are performed: 1) checking the initial value or a previously checked number, producing a checked number, to determine whether the checked number is a prime number and (determination of primacy), and if the checked number is a prime, storing an index, which refers to a plurality of numbers, which have been checked with respect to their property of being prime; and 2) selecting, when the number is not a prime number, another number based on the checked number and the index, the checked number being increased by a prescribed number; where the method further comprises the steps of: erasing a used prime number after the communication key pair has been formed; and forming, with the index and the initial value, a new communication key pair for forming the secret communication key.

15 The inventive methods and associated apparatus are described in more detail below.

16 In an embodiment of the invention, a hash function is applied to the initial value, providing a value being formed that is finally used for the key generation. Furthermore, additional data, which preferably characterize the user himself, can be used during the key generation. The RSA method for the key generation is preferably used for forming the cryptographic key. The method according to the MD-5 standard, the MD-2 standard or the Data Encryption Standard (DES) can be used as a hash function. The communication key pair can be used for enciphering or for securing the integrity of electronic data, for forming a digital signature via electronic data or for authenticating a user-- generally for any arbitrary cryptographic operation using the "Public-Key-Technology" that uses the formed communication key pair.

17 For accelerating the method, it is advantageous in an embodiment to store an index (accelerating code) when the private key is formed. The accelerating code indicates how often numbers - proceeding from the initial value - have been checked to the effect whether or not the respective number is a prime number. The method according to Miller-Rabin is preferably used for checking the property whether a number represents a prime number.

BRIEF DESCRIPTION OF THE DRAWINGS

18 An exemplary embodiment of the invention is shown in the Figures and is subsequently explained in greater detail.

Figure 1 is a flow diagram representing the method steps of the exemplary embodiment;

Figure 2 is a block diagram representing a computer network having a plurality of computers coupled to one another; and

Figure 3 is a symbolic block drawing representing the course of action for determining a prime number on the basis of an initial value.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

19 Figure 2 shows a plurality of computers 200, 210, 220, 230, 240, 250, which are connected to one another via a communication network 260. Each computer 200, 210, 220, 230, 240, 250 respectively has a plurality of input devices, i.e., a keyboard 206, 216, 226, 236, 246, 256, a mouse 207, 217, 227, 237, 247, 257, a scanner (not shown) or a camera (not shown). The entered information is supplied to a memory 202, 212, 222, 232, 242, 252 via the respective input device via an input interface/output interface 201, 211, 221, 231, 241, 251 and is stored. The 202, 2212, 222, 232, 242, 252 memory is connected to the input interface/output interface 201, 211, 221, 231, 241, 251 via a bus 204, 214, 224, 234, 254. A processor 203, 213, 223, 233, 243, 253, which is set up such that the following methods steps can be carried out, is also connected to the bus 204, 214, 224, 234, 254.

20 The computer 200, 210, 220, 230, 240, 250 communicate via the communication network 260 according to the Transport Control Protocol/Internet Protocol (TCP/IP). The communication network 260 also contains a certification unit 270 with which a certificate is prepared respectively for a public key, so that the public key is trustworthy for a communication on the basis of the "Public-Key-Technology". A user 280 enters an arbitrary prescribable word (PIN, password), which is only known to the user, into a first computer 200 (step 101, compare Figure 1).

21 According to the RSA method, the first computer 200 generates an asymmetric cryptographic key pair, as described in the following. The value 102 entered by the user 280 and additional data 103 characterizing the user 280, such as user name, personal number, terminal address etc., are supplied to a hash function (step 104). The hash function is defined and has properties as described above. The value formed by the hash function is used as a base value BW for forming two prime numbers, as symbolically shown in Figure 3. As shown in Figure 3, it is respectively checked for a value Wi (i = 1, ..., n) in an iterative method, on the basis of the base value BW, whether or not the respective value represents a prime number (step 301).

22 The method according to Miller-Rabin is utilized as method for checking the property prime for a number (see Menezes). If the number is determined to not be

prime, the number is increased by a prescribable value, preferably by the value 2 (step 302) and the test with respect to the property "prime" is repeated (step 301). This course of action is repeated until two prime numbers - a first prime number p and a second prime number q - have been determined.

23 A number, referred to as an index, indicates how often - on the basis of the base value BW- the number must be increased by the prescribed value until the first prime number p or the second prime number q is obtained. The result of the method shown in Figure 3 is two prime numbers p and q, which are used for the key generation according to the RSA method (step 105). The prime numbers p and q normally have a length of a multiple of 100 bits. A modulus n is formed from the prime numbers p and q according to the following rule:

$$n = p * q. \quad (1)$$

24 Furthermore, an intermediate variable $\varphi(n)$ is formed according to the following rule:

$$\varphi(n) = (p-1) * (q-1). \quad (2)$$

25 A secret key d is now selected such that the secret key d is relatively prime with respect to $\varphi(n)$. A public key e is determined such that the following rule is fulfilled:

$$e * d \bmod \varphi(n) = 1. \quad (3)$$

26 The value d is the private key and is not allowed to be made known to a third party. A private key d (step 106) and a public key e (step 107) have been formed as a result of the key generation (key 105). The two keys d, e form a cryptographic key pair corresponding to one another, this key pair being used for an arbitrary cryptographic operation, i.e., for enciphering, deciphering, for a digital signature, or for authenticating (step 108).

27 After the key pair d, e has been formed according to the above-described method, the private key d is erased. The public key e is supplied to the certification entity 280. A certificate Certe is formed by the certification entity 280 via the public key e and the certificate Certe of the public key e is stored in a directory 290 that can be accessed by the public. Therefore, each communication participant in the communication network 280 can access the public key e via the certificate Certe of the public key e. The secrete key d corresponding to the public key e is erased in the first computer 200.

28 Every time that the user 280 wishes to initial a communication on the basis of the key pair or when the user 280 wishes to carry out a cryptographic operation upon utilization of such a key pair, the user 280 enters his initial value (PIN, password) into the first computer 200 and the initial value 102 (as described above), in turn, is provided with additional data 103. It is then subjected to a hash function (step 104) and, on the basis of the base value BW, two prime numbers p and q are determined or a stored index (as described above) is read out or is also entered by the user 280 and a secret communication key is formed from it, which, however, corresponds to the private previously formed key d, which has been erased again.

29 In this way, a communication key pair has been formed, which comprises the secret communication key and the corresponding public key e. For a communication session, a user can thus respectively immediately generate the secret communication code, so that it is possible to use intense "Public-Key-Technology" without having to store the secret key on a chip card. The generated communication key pair d, e is used for enciphering plaintext 109 with the public key e and for deciphering the electronic, enciphered data 110 with the secret communication key.

30 Figure 1 symbolically shows the processing of plaintext 109, i.e., electronic data 109 that can be read by everybody, as well as enciphered electronic data 110, where the communication device is respectively described by an arrow toward or from the block representing a cryptographic operation 108.

31 The enciphering or, respectively, deciphering is performed according to the following rules:

$$m^e \bmod n = c, \qquad (4)$$

where

- m refers to a quantity of 512 bit of electronic data 109 to be enciphered,
- c refers to enciphered electronic data 110.

32 The deciphering of the enciphered electronic data c is performed according to the following rule:

$$m = c^d \bmod n. \qquad (5)$$

33 A few alternatives of the above-described exemplary embodiment are explained as follows. The method can be used for enciphering, for securing integrity and for a digital signature of electronic data. Furthermore, the invention can be utilized in the field of secure electronic mail systems. The user must not necessarily enter the initial value 102 during the generation of the key pair at the beginning of the method, but a central unit generating the key pair can prescribe it to the user. Therefore, the user must merely remember a password or a PIN, and it is no longer necessary to securely store a secret cryptographic key, for example, on a chip card, which is associated with corresponding risks and with considerable outlay. Instead of a hash function, any arbitrary one-way function can be used in the framework of the invention.

34 The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.

ABSTRACT

After a key pair with a public key and a corresponding private key has been determined on the basis of an initial value, the initial value is made available to a user. The private key can then be erased. When the user wishes to carry out a cryptographic operation based on the "Public-Key-Technology", the user enters the initial value into a computer and, upon utilization of the initial value, a secret communication key is formed, which corresponds to the private key that had been previously formed but was then erased.

METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

The invention relates to a method and an arrangement for forming a secret communication key for a predetermined asymmetric key pair.

The formation of an asymmetric cryptographic key pair is known from [1].

Given this method, the RSA method for forming a cryptographic key pair, which comprises a secret key and a corresponding public key, is formed.

Only the user knows the secret key; the public key can be made known to all subscribers of a communication network.

The user signs the data with his secret key when a digital signature is prepared for protecting the authenticity and integrity of electronic data. The signed digital signature is verified upon utilization of the public key corresponding to the secret key, so that the authenticity or, respectively, integrity of the digital signature can be checked by all communication partners, which have access to the public key.

The aforementioned what is referred to as "Public-Key-Technology" is particularly applied in the digital communication within a computer network (a fixed number of computer units, which are connected to one another via a communication network).

Given the method known from [1], the protection of the secret key against unauthorized access of a third party is of critical importance for the security of the digital signature.

It is known from [2] to store the secret key on an external medium for storing data, for example a chip card, a disk etc., or on a hard disk, whereby key data are protected in that a personal identification code (Personal Identification Number, PIN) or a password, with which the key data are respectively deciphered is used. It is necessary, however, to access the local resources of a user when these external media are used. This is not desired especially with respect to a network-oriented infrastructure of network computers or Java applications.

A network computer is a computer, which is networked with other computers.

A Java application is a program containing programs that are written in the programming language Java.

Therefore, the method known from [2] is associated with the disadvantage that the secret key must be stored on an external medium, so that it is very difficult to protect the secret key against misuse.

An overview regarding hash functions can be found in [3]. A hash function is a function, wherein it is possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function. Such an additional property is collision freedom, i.e., it is not allowed to be possible to find two different input character strings resulting in the same output character string.

Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

A method referred to as a method according to Miller-Rabin, wherein it can be checked for a number whether it is a prime number, is known from [4].

Therefore, an object of the invention is to form a secret communication key for a predetermined asymmetric cryptographic key pair, wherein the secret key of the asymmetric key pair must not be stored permanently.

The problem is solved by the method and by the arrangement with the features of the independent patent claims.

Given the method for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a secret key and a corresponding public key, a prescribable initial value has been used with respect to the determination of the key pair. The initial value is available to a user. The user enters the initial value into the computer and the secret communication key is formed upon utilization of the initial value. The secret communication key and the public key form a communication key pair.

The arrangement for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a secret key and a corresponding public key, has a processor, which is set up such that the following steps can be carried out:

- a prescribed initial value has been used for determining the key pair,
- the user enters the initial value into the computer,
- the secret communication key is formed upon utilization of the initial value, whereby the secret communication key and the public key form a communication key pair.

Furthermore, an input means is provided for entering the initial value by the user.

As a result of the invention, it is possible to erase the secret key without having to forego the intense cryptography of the "Public-Key-Technology".

Concretely, the initial value can be regarded as a personal identification code (Personal Identification Number PIN) or as a password that is prescribed by the user or that is centrally prescribed and that is entered by the user into the computer. After the password or, respectively, the PIN has been entered, the secret communication key, i.e. the key that is of the same name compared to the secret key, is formed, which forms a key pair, the communication key pair, together with the public key, upon utilization of the the [sic] password or, respectively, of the PIN as an initial value. [sic]

In this way, a fusion of the password technology customary to the user of a conventional computer network or, respectively, of a conventional computer with the intense cryptology is inventively achieved without considerable efforts being necessary in order to permanently store secret key material.

Preferred embodiments of the invention derive from the dependent claims.

In an embodiment of the invention, a hash function is applied to the initial value, whereby a value is formed that is finally used for the key generation.

Furthermore, additional data, which preferably characterize the user himself, can be used during the key generation.

The RSA method for the key generation is preferably used for forming the cryptographic key.

The method according to the MD-5 standard, the MD-2 standard or the Data Encryption Standard (DES) can be used as hash function can be used [sic].

The communication key pair can be used for enciphering or for securing the integrity of electronic data, for forming a digital signature via electronic data or for

authenticating a user, generally for any arbitrary cryptographic operation using the "Public-Key-Technology", whereby the formed communication key pair is utilized.

For accelerating the method, it is advantageous in an embodiment to store an index when the secrete key is formed, which index is referred to as accelerating code in the following. The accelerating code indicates how often numbers - proceeding from the initial value - have been checked to the effect whether or not the respective number is a prime number.

The method according to Miller-Rabin is preferably used for checking the property whether a number represents a prime number.

An exemplary embodiment of the invention is shown in the Figures and is subsequently explained in greater detail.

Shown are

Figure 1 a flow diagram representing the method steps of the exemplary embodiment;

Figure 2 a drawing representing a computer network having a plurality of computers coupled to one another;

Figure 3 a symbolic drawing representing the course of action for determining a prime number on the basis of an initial value.

Figure 2 shows a plurality of computers 200, 210, 220, 230, 240, 250, which are connected to one another via a communication network 260. Each computer 200, 210, 220, 230, 240, 250 respectively has a plurality of input means, i.e. a keyboard 206, 216, 226, 236, 246, 256, a mouse 207, 217, 227, 237, 247, 257, a scanner (not

shown) or a camera (not shown). The entered information is supplied to a memory 202, 212, 222, 232, 242, 252 via the respective input means via an input interface/output interface 201, 211, 221, 231, 241, 251 and is stored. The 202, 2212, 222, 232, 242, 252 memory is connected to the input interface/output interface 201, 211, 221, 231, 241, 251 via a bus 204, 214, 224, 234, 254. A processor 203, 213, 223, 233, 243, 253, which is set up such that the following methods steps can be carried out, is also connected to the bus 204, 214, 224, 234, 254.

The computer 200, 210, 220, 230, 240, 250 communicate via the communication network 260 according to the Transport Control Protocol/Internet Protocol (TCP/IP).

The communication network 260 also contains a certification unit 270 with which a certificate is prepared respectively for a public key, so that the public key is trustworthy for a communication on the basis of the "Public-Key-Technology".

A user 280 enters an arbitrary prescribable word (PIN, password), which is only known to the user, into a first computer 200 (step 101, compare **Figure 1**).

According to the RSA method, the first computer 200 generates an asymmetric cryptographic key pair, as described in the following.

The value 102 entered by the user 280 and additional data 103 characterizing the user 280, such as user name, personal number, terminal address etc., are supplied to a hash function (step 104).

[3] contains an overview regarding hash functions. A hash function is a function, wherein it is not possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function. Such an additional property is collision freedom, i.e.,

it is not allowed to be possible to find two different input character strings resulting in the same output character string.

Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

The value formed by the hash function is used as base value BW for forming two prime numbers, as symbolically shown in **Figure 3.**

As shown in **Figure 3**, it is respectively checked for a value Wi (i = 1, ..., n) in an iterative method, on the basis of the base value BW, whether or not the respective value represents a prime number (step 301).

The method according to Miller-Rabin is utilized as method for checking the property prime for a number (see [4]).

If it is determined for a number that the number does not represent a prime number, the number is increased by a prescribable value, preferably by the value 2 (step 302) and the test with respect to the property "prime" is repeated (step 301). This course of action is repeated until two prime numbers - a first prime number P and a second prime number q - have been determined.

Referred to as index is a number indicating how often - on the basis of the base value PW [sic] - the number must be increased by the prescribed value until the first prime number p or, respectively, the second prime number q is obtained.

The result of the method shown in **Figure 3** is two prime numbers p and q, which are used for the key generation according to the RSA method (step 105).

The prime numbers p and q normally have a length of a plurality of 100 bit.

A modulus n is formed from the prime numbers p and q according to the following rule:

$$n = p * q. \quad (1)$$

Furthermore, an intermediate variable $\varphi(n)$ is formed according to the following rule:

$$\varphi(n) = (p-1) * (q-1). \quad (2)$$

A secret key d is now selected such that the secret key d is relatively prime with respect to φ (n). A public key e is determined such that the following rule is fulfilled:

$$e * d \text{ mop } \varphi(n) = 1. \quad (3)$$

The value d is the secret key and is not allowed to make known to a third party.

Therefore, a private key d (step 106) and a public key e (step 107) have been formed as a result of the key generation (key 105).

The two keys d, e form a cryptographic key pair corresponding to one another, this key pair being used for an arbitrary cryptographic operation, i.e. for enciphering, deciphering, for the digital signature or for authenticating (step 108).

After the key pair d, e has been formed according to the above-described method, the secret key d is erased.

The public key e is supplied to the certification entity 280. A certificate Certe is formed by the certification entity 280 via the public key e and the certificate Certe of the public key e is stored in a directory 290 that can be accessed by the public.

Therefore, each communication participant in the communication network 280 can access the public key e via the certificate Certe of the public key e.

The secrete key d corresponding to the public key e is erased in the first computer 200.

Every time when the user 280 wishes to initial a communication on the basis of the key pair or, respectively, when the user 280 wishes to carry out a cryptographic operation upon utilization of such a key pair, the user 208 [sic] enters his initial value (PIN, password) into the first computer 200 and the initial value 102 (as described above), in turn, is provided with additional data 103, is subjected to a hash function (step 104) and, on the basis of the base value BW, two prime numbers p and q are determined or a stored index (as described above) is read out or is also entered by the user 280 and a secrete communication key is formed therefrom, which, however, corresponds to the secrete, previously formed key d, which has been erased again.

In this way, a communication key pair has been formed, which comprises the secrete communication key and the corresponding public key e. For a communication session, a user can thus respectively currently generate the secrete communication code, so that it is possible to use intense "Public-Key-Technology" without having to store the secrete key on a chip card.

The thus generated communication key pair d, e is used for enciphering plaintext 109 with the public key e and for deciphering the electronic, enciphered data 110 with the secrete communication key.

Figure 1 symbolically shows the processing of plaintext 109, i.e., electronic data 109 that can be read by everybody, as well as enciphered electronic data 110, whereby the communication device respectively describes by an arrow toward or, respectively, from the block representing a cryptographic operation 108. [sic]

The enciphering or, respectively, deciphering is performed according to the following rules:

$$m^e \bmod n = c, \qquad (4)$$

whereby

- m refers to a quantity of 512 bit of electronic data 109 to be enciphered,
- c refers to enciphered electronic data 110.

The deciphering of the enciphered electronic data c is performed according to the following rule:

$$m = c^d \bmod n. \qquad (5)$$

A few alternatives of the above-described exemplary embodiment are explained in the following:

The method can be used for enciphering, for securing integrity and for the digital signature of electronic data.

Furthermore, the invention can be utilized in the field of secure electronic mail systems.

The user must not necessarily enter the initial value 102 during the generation of the key pair at the beginning of the method, but a central unit generating the key pair can prescribe it to the user.

Therefore, the user must merely remember a password or, respectively, a PIN and it is no longer necessary to securely store a secrete cryptographic key, for example on a chip card, this being associated with corresponding risks and with considerable outlay.

Instead of a hash function, any arbitrary one-way function can be used in the framework of the invention.

The following publications have been cited in the framework of this document.

[1] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 79 - 85, 1993

[2] D. Longley and M. Shain, Data & Computer Security, Dictionary of standards concepts and terms, Stockton Press, ISBN 0-333-42935-4, page 317, 1987

[3] [1] C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 68 - 73, 1993

[4] A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN 0-8493-8523-7, page 138 - 140, 1997

Patent claims

1. Method for forming a secrete communication key for a predetermined asymmetric cryptographic key pair, which comprises a secrete key and a corresponding public key, by a computer,

a) whereby a prescribable initial value has been used given the determination of the key pair,

b) whereby the initial value is made available to a user,

c) whereby the user enters the initial value into the computer,

d) whereby the secrete communication key is formed upon utilization of the initial value, whereby the secrete communication key and the public key form an asymmetric cryptographic communication key pair.

2. Method according to claim 1,
whereby the initial value is supplied to a hash function and the value formed by the hash function is used for determining the key pair and the communication key pair.

3. Method according to claim 1 or 2,
whereby additional data characterizing the user are utilized when the key pair and the communication key pair are formed.

4. Method according to one of the claims 1 to 3,

- whereby a prime number is determined on the basis of the initial value, whereby, in an iterative method, it is checked whether the respectively checked number is a prime number and when this is the case, an index is stored, which refers to a plurality of numbers, which have been checked with respect to their property whether they are a prime number, is stored [sic],
- otherwise, another number is selected on the basis of the checked number and the index is increased by a prescribed number,

- whereby the used prime number is erased after the communication key pair has been formed,

whereby the index and the initial value are respectively used for forming a new communication key pair for forming the secrete communication key.

5. Method according to claim 4,

whereby the test, whether a number is a prime number, is carried out according to the method of Miller-Rabin.

6. Method according to one of the claims 1 to 5,

whereby the keys are formed according to the RSA method.

7. Method according to one of the claims 2 to 6,

whereby the hash function is one of the following methods:

- MD-5 method,
- MD-2 method,
- the method according to the Data Encryption Standard (DES) as one-way function.

8. Method according to one of the claims 1 to 7,

used for enciphering electronic data with the secrete communication key.

9. Method according to one of the claims 1 to 7,

used for forming a digital signature via electronic data upon utilization of the secrete communication key.

10. Method according to one of the claims 1 to 7,

used for authenticating upon utilization of the secrete communication key.

11. Arrangement for forming a secrete communication key for a predetermined asymmetric cryptographic key pair, which comprises a secrete key and a

corresponding public key, with a processor being set up such that the following steps can be carried out:

- the key pair has been determined upon utilization of a prescribable initial value,
- the initial value is made available to a user,
- the user enters the initial value into the computer,
- the secrete communication key is formed upon utilization of the initial value, whereby the secrete communication key and the public key form a communication key pair, and

with an input means for entering the initial value by the user.

12. Arrangement according to claim 11,
whereby the processor is set up such that the initial value is supplied to a hash function and the value formed by the hash function is used for determining the key pair and the communication key pair.

13. Arrangement according to claim 11 or 12,
whereby the processor is set up such that additional data characterizing the user are utilized during the formation of the key pair and the communication key pair.

14. Arrangement according to one of the claims 11 to 13,
whereby the processor is set up such that

- a prime number is determined on the basis of the initial value, whereby, in an iterative method, it is checked whether the respectively checked number is a prime number and when this is the case, an index is stored, which refers to a plurality of numbers, which have been checked with respect to their property whether they are a prime number, is stored [sic],
- otherwise, another number is selected on the basis of the checked number and the index is increased by a prescribed number,
- whereby the used prime number is erased after the communication key pair has been formed,

- whereby the index and the initial value are respectively used for forming a new communication key pair for forming the secrete communication key.

15. Arrangement according to claim 14,
whereby the processor is set up such that the test, whether a number is a prime number, is performed according to the method of Miller-Rabin.

16. Arrangement according to one of the claims 11 to 15,
whereby the processor is set up such that the keys are formed according to the RSA method.

17. Arrangement according to one of the claims 12 to 16,
whereby the processor is set up such that the hash function is one of the following methods
. Method according to one of the claims 2 to 6,
whereby the hash function is one of the following methods:
- MD-5 method,
- MD-2 method,
- the method according to the Data Encryption Standard (DES) as one-way function.

18. Method according to one of the claims 11 to 17,
used for enciphering electronic data with the secrete communication key.

19. Arrangement according to one of the claims 11 to 17,
used for forming a digital signature via electronic data upon utilization of the secrete communication key.

20. Arrangement according to one of the claims 11 to 17,
used for authenticating upon utilization of the secrete communication key.

Abstract

Method and arrangement for forming a secrete communication key for a predetermined asymmetric cryptographic key pair

After a key pair with a public key and a corresponding secrete key has been determined on the basis of an initial value, the initial value is made available to a user. The secrete key can be erased. When the user wishes to carry out a cryptographic operation based on the "Public-Key-Technology", the user enters the initial value into a computer and, upon utilization of the initial value, a secrete communication key is formed, which corresponds to the secrete key previously formed but erased since.

Sign. Figure 1

FIG 1

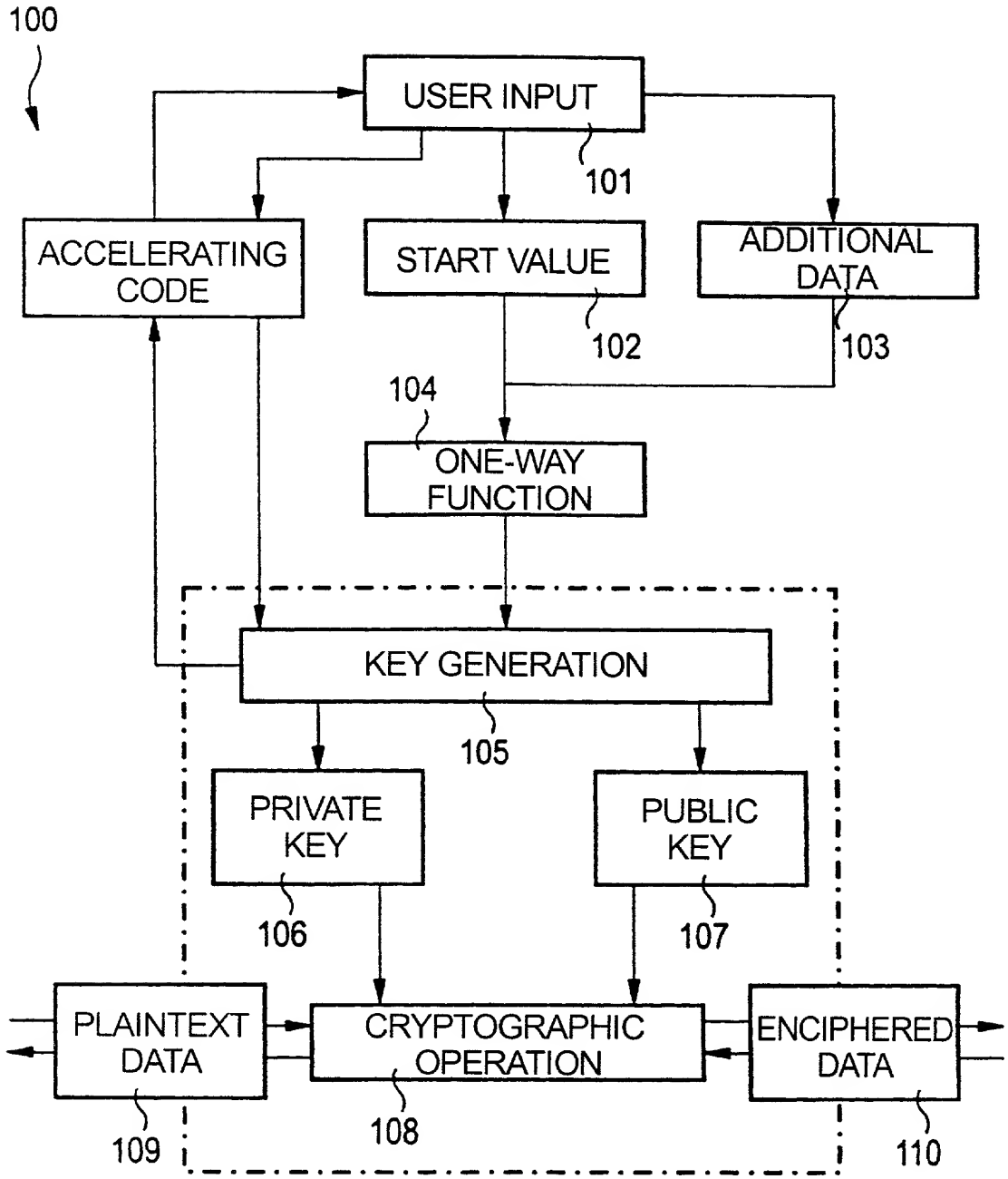

100
USER INPUT
101
ACCELERATING CODE
START VALUE
ADDITIONAL DATA
102
103
104
ONE-WAY FUNCTION
KEY GENERATION
105
PRIVATE KEY
PUBLIC KEY
106
107
PLAINTEXT DATA
CRYPTOGRAPHIC OPERATION
ENCIPHERED DATA
109
108
110

FIG 2

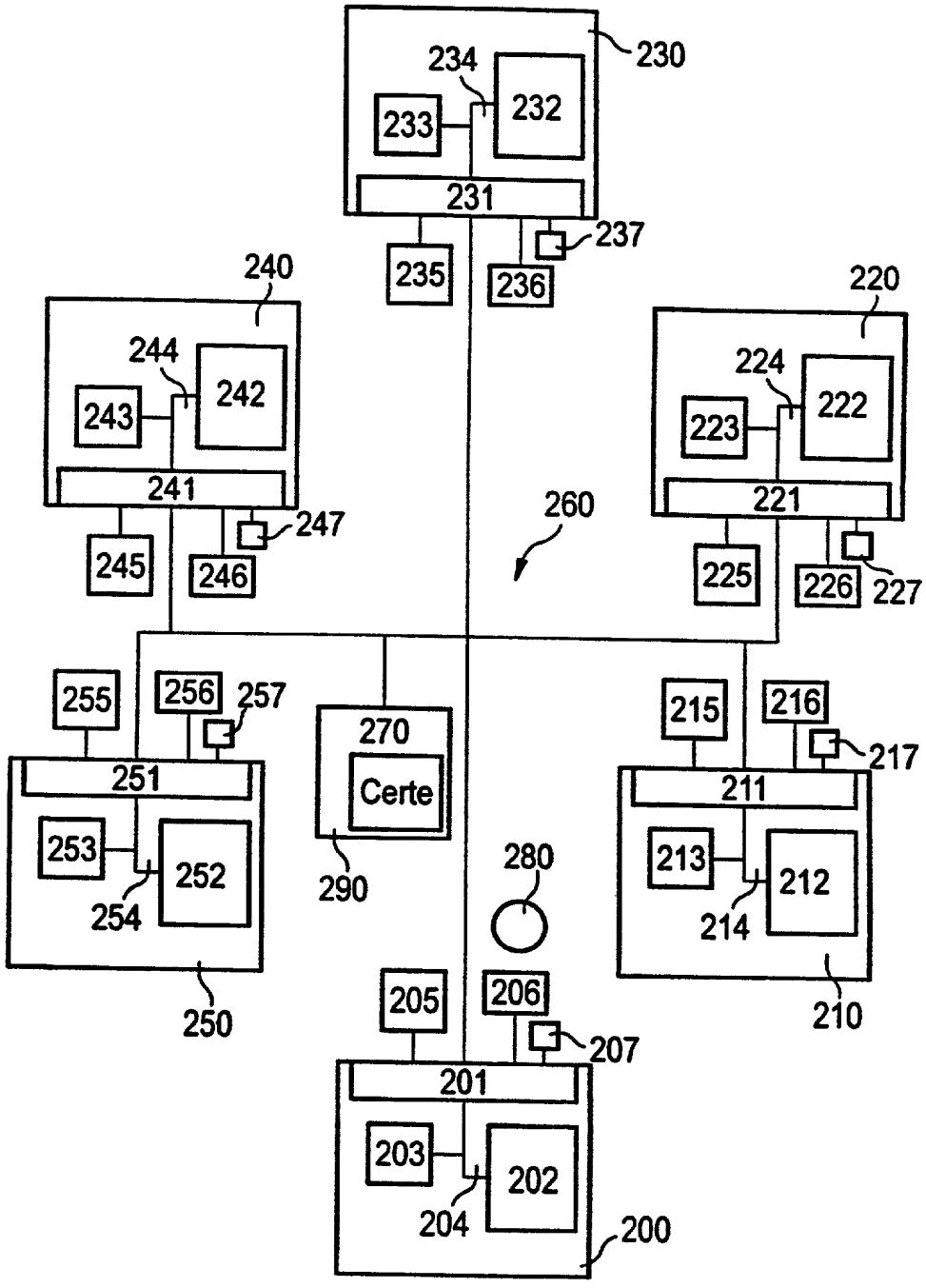
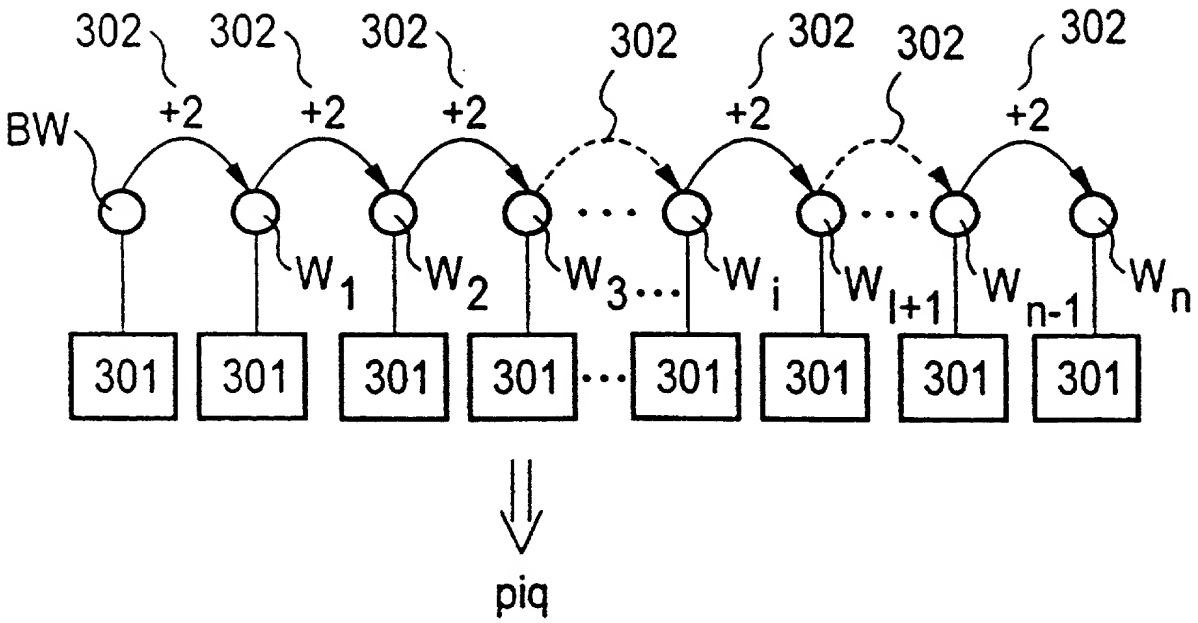

230
234
232
233
231
237
235
236
240
220
244
242
243
241
247
245
246
224
222
223
221
260
225
226
227
255
256
257
270
Certe
215
216
217
251
253
252
254
290
280
211
213
212
214
205
206
207
250
210
201
203
202
204
200

FIG 3


302
302
302
302
302
302
302
+2
+2
+2
+2
+2
+2
BW
W1
W2
W3
Wi
WI+1
Wn-1
Wn
301
301
301
301
301
301
301
301
piq

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Verfahren und Anordnung zur Bildung eines geheimen Kommunikationsschlüssels zu einem zuvor ermittelten asymmetrischen kryptographischen Schlüsselpaar

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)

(check one)

☒ hier beigefügt ist.

☒ is attached hereto.

☐ am _____ als PCT internationale Anmeldung PCT Anmeldungsnummer _____ eingereicht wurde und am _____ abgeändert wurde (falls tatsächlich abgeändert).

☐ was filed on _____ as PCT international application PCT Application No. _____ and was amended on _____ (if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Priorität beansprucht

			Priority Claimed	
198 37 405.4	Germany	18. August 1998	☒	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

BOX PCT
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

CHANGE OF ADDRESS OF APPLICANTS' REPRESENTATIVE

APPLICANT(S):	GERHARD HOFFMANN ET AL
ATTORNEY DOCKET NO.:	P00,1996
INTERNATIONAL APPLICATION NO:	PCT/DE99/02443
INTERNATIONAL FILING DATE:	04 AUGUST 1999
INVENTION:	METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

Assistant Commissioner for Patents,
Washington D.C. 20231

S I R:

Members of the firm of Hill & Simpson designated on the original Power of Attorney have merged into the firm of Schiff Hardin & Waite. All future correspondence for the above-referenced application therefore should be sent to the following address:

SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6473

CUSTOMER NUMBER 26574

Submitted by,

Mark Bergner (Reg. No. 45,877)

Mark Bergner
SCHIFF HARDIN & WAITE
Patent Department
6600 Sears Tower
Chicago, Illinois 60606-6473
Telephone: (312) 258-5779
Attorneys for Applicants
CUSTOMER NUMBER 26574

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 9/30, 9/08, 9/32

A1

(11) Internationale Veröffentlichungsnummer: **WO 00/11833**

(43) Internationales Veröffentlichungsdatum: 2. März 2000 (02.03.00)

(21) Internationales Aktenzeichen: PCT/DE99/02443

(22) Internationales Anmeldedatum: 4. August 1999 (04.08.99)

(30) Prioritätsdaten:
198 37 405.4 18. August 1998 (18.08.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HOFFMANN, Gerhard [DE/DE]; Gozbertstr. 8/II, D–81547 München (DE). LUKAS, Klaus [DE/DE]; Niemöllerallee 6, D–81739 München (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND DEVICE FOR CREATING A SECRET COMMUNICATION KEY FOR A PREDETERMINED ASYMMETRIC AND CRYPTOGRAPHIC KEY-PAIR

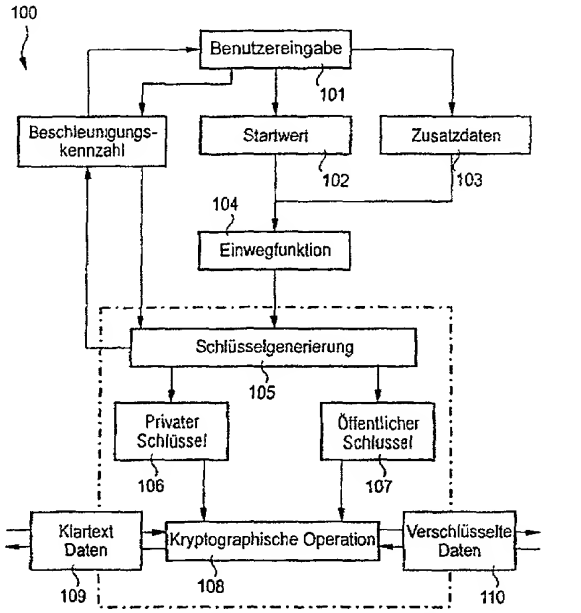
(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR BILDUNG EINES GEHEIMEN KOMMUNIKATIONSSCHLÜSSELS ZU EINEM ZUVOR ERMITTELTEN ASYMMETRISCHEN KRYPTOGRAPHISCHEN SCHLÜSSELPAAR

(57) Abstract

The present invention involves determining a pair of keys comprising a public key and a corresponding secret key from an initial value, and sending this initial value to an user. The secret key can be erased. If the user wants to carry out a cryptographic operation based on the public–key techniques, said user inputs the initial value into a computer and, thanks to said initial value, receives a secret communication key that corresponds to the secret key previously generated but erased since.

(57) Zusammenfassung

Nachdem ein Schlüsselpaar mit einem öffentlichen Schlüssel und einem korrespondierenden geheimen Schlüssel ausgehend von einem Startwert ermittelt wurde, wird der Startwert einem Benutzer zur Verfügung gestellt. Der geheime Schlüssel kann gelöscht werden. Wenn der Benutzer eine auf der Public–Key–Technologie basierende kryptographische Operation durchführen möchte, gibt der Benutzer den Startwert in einen Rechner ein und unter Verwendung des Startwerts wird ein geheimer Kommunikationsschlüssel gebildet, der dem zuvor gebildeten, seitdem gelöschten geheimen Schlüssel entspricht.



German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Messrs. John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

312/876-0200
Ext. _____

Postanschrift:

Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders: HOFFMANN, Gerhard	Full name of sole or first inventor:
Unterschrift des Erfinders: Gerhard Hoffmann Datum: 29.07.99	Inventor's signature Date
Wohnsitz: D-81547 München, Germany DE	Residence
Staatsangehörigkeit: Bundesrepublik Deutschland	Citizenship
Postanschrift: Gozbertstr. 8/II D-81547 München Bundesrepublik Deutschland	Post Office Addess
Voller Name des zweiten Miterfinders (falls zutreffend): LUKAS, Klaus	Full name of second joint inventor, if any:
Unterschrift des Erfinders: Klaus Lukas Datum: 11.06.65	Second Inventor's signature Date
Wohnsitz: D-81739 München, Germany DE	Residence
Staatsangehörigkeit: Bundesrepublik Deutschland	Citizenship
Postanschrift: Niemöllerallee 6 D-81739 München Bundesrepublik Deutschland	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Form PTO-FB-240 (8-83) Patent and Trademark Office-U.S. Department of COMMERCE